



# Hardening Joomla! (MNI)

Web Security SS10

Supervised by: Prof. Dr. Klaus Quibeldey-Cirke

# Content

- \* Introduction
- \* Giessen Aegis
- \* Suhosin
- \* Security Tests: OWASP-Top Ten Risks
- \* Livedemo
- \* Conclusion

# Introduction

- \* Project Goal: Implementation of a security architecture for Joomla!(1.5)
- \* Assignments:
  - \* Integration of PHPIDS
  - \* Implementation of an IPS
  - \* Statistical Analysis
  - \* Tests with Jmeter
  - \* Integration of Suhosin
  - \* SecurityTests based on the OWASP Top 10 Security Risks

# Giessen Aegis

- \* Plugin `plg_giessenAegis`
- \* ReCaptcha
- \* Component `com_giessenAegis`
- \* Module `mod_giessenAegis`
- \* Tests with Jmeter
- \* Additional backend module `mod_phpConfigCheck`

# Plugin plg\_giessenAegis

- \* PHPIDS calculates impact based on user activities
- \* This threshold is used for countermeasure selection
- \* These countermeasures include:
  - \* Logging
  - \* Email-Notification
  - \* User Warnings
  - \* User Logout
  - \* Restriction of User Access

# Plugin plg\_giessenAegis

- \* Log Files and Email Notifications Contain:
  - \* User ID/IP
  - \* Date
  - \* URL of the Page Being Accessed
  - \* Impact (PHPIDS-Threat Level)
  - \* User Entry
  - \* HTTP Method Used (GET/POST/...)
  - \* Attack Vectors (xss/csrf/id/...)
  - \* Plain Text Description of the Attack

# Plugin plg\_giessenAegis

- \* ..Makes Use of Other Functionality:
  - \* Should com\_giessenaegis be installed, attack properties are saved in database tables as well as in the log file.
  - \* White Lists: Exceptions to security rules can be created for front end (public) as well as backend (administrator) areas.

# Plugin plg\_giessenAegis

- \* ... Makes Use of Other Functionality:
  - \* Updates PHP IDS filter lists
  - \* A simulation mode can be turned on (IPS is then deactivated)
  - \* Display of data from the log file
  - \* Deletion of the log file or database entries
  - \* Selectable warning type (URL entry for redirection, plain text, or escalating levels of displays for the user)



# Plugin plg\_giessenAegis

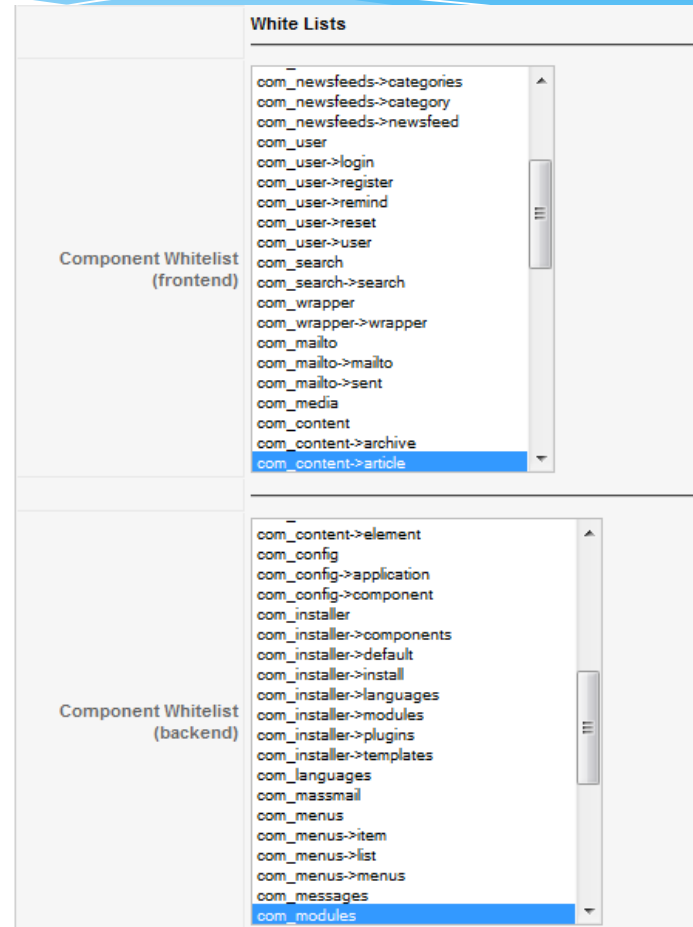
## Backend:

PHP IDS Version	Check for version updates?
<b>Intrusion Prevention System</b>	
IPS	active
<b>Dependencies</b>	
auto_update	Element not defined for type = giessenAegisautoupdate
Component Status	
<b>Countermeasure Thresholds</b>	
Activity Time	5
Log	3
Mail	9
Warnung	27
Abmelden	50
Ban	100
<b>Countermeasure Specific Settings</b>	
Warning Type	Escalating Counter Measure Messages
Special Display URL	plugins/system/giessenAegis/Gegenm1/hard.php
Warning Text	Aufgrund Ihrer Aktivitäten wurden Sie als Angreifer identifiziert. Jede weitere verdächtige Aktivität
Mail Recipients	Administrator wng74

<b>Log Settings</b>	
Select a date	2010-09-09
	Current Size: 57.30 KB
Log File	
	Current number of rows: 34
Log DB	
<b>reCaptcha Settings</b>	
Public Key	
Private Key	
Request Threshold	10
Avg Request Time	3

# Plugin plg\_giessenAegis

Backend:



# ReCaptcha

- \* Countermeasure: **reCaptcha**
  - \* Protects against automated attacks and crawlers
  - \* Captcha is activated by too many requests in too short a time period
    - \* For example: the average time of request reception from a particular IP for 10 requests is less than 3 seconds
  - \* The use of the captcha is required to further access the site
  - \* Realization by means of the Zend Framework

# ReCaptcha

## reCaptcha Display

Name  Passwort  Angemeldet bleiben ☐ Login   1 (0) Suchen

**MNI**  
FH GIESSEN-FRIEDBERG

Startseite Studium Forschung & Weiterbildung Fachbereich Lernplattform

QuickLinks

rise

sinkers

Type the two words:



  
stop spam.  
read books.

# com\_giessenAegis Component

- \* Serves the execution of statistical analysis
- \* Makes use of two database tables
  - \* Entries for discovered attacks
  - \* Plain text resolution of possible attack vectors
- \* 3 Backend Views
  - \* Statistics
  - \* Management
  - \* Attack Types

# com\_giessenAegis Component

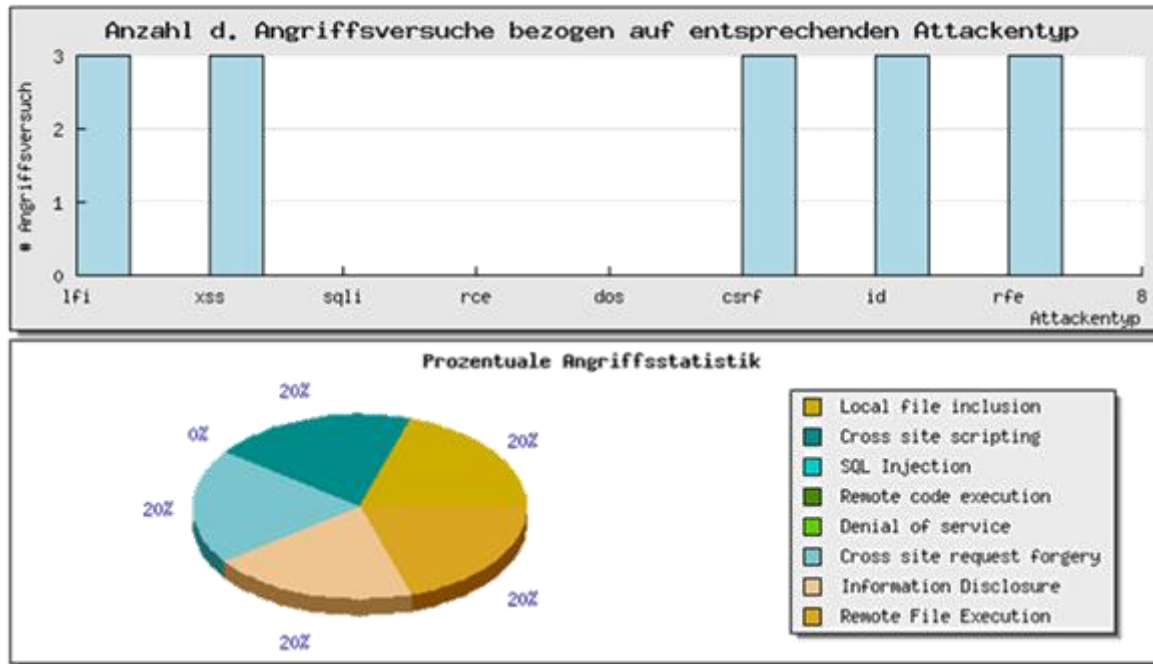
- \* **Statistical Analysis:**

- \* Various Statistics for Logged Attacks
  - \* Amount of different attacks
  - \* Percent of Attacks by Attack Type
  - \* Statistical Analysis of Attacks by Specific Users
- \* Statistics are dynamically analyzed, created, and displayed using [JPGraph](#)
- \* Statistics can be (de)activated individually
- \* Time frame for analysis of individual statistics can be set

# com\_giessenAegis Component

Backend:

Angezeigter Zeitraum: 06.09.2010 - 23.11.2010



# com\_giessenAegis Component

Backend:

**Giessen Aegis** [Speichern] [Abbrechen]

**Konfiguration**

	<b>Anzahl der Angriffe bezogen auf entsprechende Attackentypen</b>
Graph anzeigen	<input checked="" type="radio"/> Ja <input type="radio"/> Nein
Zeitraum (Beginn)	2010-09-06
Zeitraum (Ende)	2010-11-23

	<b>Prozentuale Angriffsstatistik</b>
Graph anzeigen	<input checked="" type="radio"/> Ja <input type="radio"/> Nein

	<b>Anteil externer/interner Angriffsversuche</b>
Graph anzeigen	<input checked="" type="radio"/> Ja <input type="radio"/> Nein
Zeitraum (Beginn)	2010-06-09
Zeitraum (Ende)	2020-06-01

**Anzahl der Angriffsversuche bezogen auf entsprechende Hosts**



# com\_giessenAegis Component

- \* Management Display:
  - \* Serves to manage individual statistics
  - \* Displays currently banned users
  - \* Banned users can be unbanned from this display

# com\_giessenAegis Component

Backend:



The screenshot shows the Joomla! Backend interface for the 'Giessen Aegis' component. The top header bar is black with the Joomla! logo and the text 'Fachbereich MNI' on the left, and 'Version 1.5.15' on the right. Below the header is a green navigation bar with tabs: Site, Menüs, Inhalt, Komponenten, Erweiterungen, Werkzeuge, and Hilfe. To the right of these tabs are icons for 'Vorschau', '0', '1', and 'Abmelden'. The main content area has a title bar with a folder icon and the text 'Giessen Aegis'. To the right of the title bar are two buttons: 'User freigeben' (with a red arrow icon) and 'Zurück' (with a green arrow icon). Below the title bar is a sub-navigation bar with tabs: 'Statistiken', 'Verwaltung' (which is underlined), and 'Attackentypen'. The main content area displays a table titled 'Gekannte User:' (Note: the image shows 'Gekannte' instead of 'Gekannte'). The table has two columns: '# Benutzer' and 'Benutzer'. The first row shows the number '1' and the username 'kneisel'.

#	Benutzer
1	kneisel

# com\_giessenAegis Component

- \* Attack Type Display:
  - \* Displays a list of attack types which PHP IDS detects
  - \* This list is predefined by PHPIDS and resides in the database
  - \* Attack Types can be:
    - \* created
    - \* edited
    - \* deleted
  - \* Serves to resolve codes for attack types  $\leftrightarrow$  plain text names

# com\_giessenAegis Component

## Backend:

Statistiken | Verwaltung | Attackentypen

Filter:

#	<input type="checkbox"/>	Attacke▲	Abkürzung	ID
1	<input type="checkbox"/>	Cross site request forgery	CSRF	6
2	<input type="checkbox"/>	Cross site scripting	XSS	2
3	<input type="checkbox"/>	Denial of service	DOS	5
4	<input type="checkbox"/>	Information Disclosure	ID	7
5	<input type="checkbox"/>	Local file inclusion	LFI	1
6	<input type="checkbox"/>	Remote code execution	RCE	4
7	<input type="checkbox"/>	Remote File Execution	RFE	8
8	<input type="checkbox"/>	SQL Injection	SQLI	3

Anzeige # 10 ▼

# mod\_giessenAegis Module

- \* The module serves the front end display of detected attacks
- \* Displays a compact view of the most recent suspected attacks
- \* More detailed information is displayed in the tooltip to the specific attack
- \* Mnemonic Display using Icons:
  - \* New Attacks → „neu“ Symbol
  - \* Particularly Malicious Attacks → Warning Symbol
- \* Many display properties can be set in the parameters to the module in the backend

# mod\_giessenAegis Module

## Frontend:



# mod\_giessenAegis Module

## Frontend:

**Giessen Aegis**

- Ext. Angriff (30.06.10 10:21:12) **neu** alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** <script>alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** **Details**  
Angriffe: xss, csrf, id, rfe, lfi  
Impact: 16
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...

**Giessen Aegis**

- Ext. Angriff (30.06.10 10:21:12) **neu** alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** <script>alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** **IP: 127.0.0.1**  
30.06.10 10:21:11 <script> ...
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...

**Giessen Aegis**

- Ext. Angriff (30.06.10 10:21:12) **neu** alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** <script>alert(); ...
- Ext. Angriff (30.06.10 10:21:11) **!** **neu** <script>alert();
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...
- Int. Angriff (11.06.10 09:23:02) **!** <input[^>]\*value=\& ...

# mod\_giessenAegis Module

## Backend:

Parameter

▼ Modulparameter

Anz.d.Attacken	<input type="text" value="5"/>
Zeichenbeschr.	<input type="text" value="25"/>
Vektor anz.	<input checked="" type="radio"/> Aktivieren <input type="radio"/> Deaktivieren
Datum anz.	<input checked="" type="radio"/> Aktivieren <input type="radio"/> Deaktivieren
New-Icon anz.	<input checked="" type="radio"/> Aktivieren <input type="radio"/> Deaktivieren
Neu ab	<input type="text" value="5"/>
New-Icon	<input type="text" value="neu_blue_12.png"/> ▼
Warning-Icon anz.	<input checked="" type="radio"/> Aktivieren <input type="radio"/> Deaktivieren
Warning ab	<input type="text" value="10"/>
Warning-Icon	<input type="text" value="warning_1.png"/> ▼



# JMeter-Tests

- \* External Attacks
  - \* SQL-Injections
  - \* XSS
- \* Internal Attacks
  - \* After Login
  - \* SQL-Injections
  - \* XSS
  - \* Attacking multiple times to simulate logout/banning

# Backend module mod\_phpConfigCheck

- \* Displays recommended php.ini options
- \* Compares with current runtime settings

► Update nötig?		
► Suhosin		
▼ phpConfigCheck		
Config Option	Current Value	Recommended Value
register_globals	off	off
save_mode	off	on
open_base_dir	off	on
display_errors	1	off
allow_url_fopen	1	off
allow_url_include	off	off

# Suhosin

- \* Inclusion
- \* Configuration
- \* Backend module `mod_suhosin`

# Suhosin-Inclusion

- \* Server is hardened against known and unknown vectors
- \* PHP update to version 5.3.3
- \* Installation of Suhosin extension and patches

# Suhosin-Configuration

- \* Customized default configuration
  - \* Customizing was done by examination of log files while using the test system
- \* Linked with ClamAV
  - \* New script to link ClamAV with Suhosin
  - \* Checks files right after upload

# Suhosin – Backend module


- \* Backend module `mod_suhosin`:
  - \* Administration of Suhosin in Joomla!'s backend
  - \* Shows if Suhosin installation is present and up to date
  - \* Switch to enable/disable simulation mode
  - \* Displays the Logfile
  - \* Displays Suhosin configuration, which can be modified

# Suhosin – Backend module

► Update nötig?

▼ Suhosin





Status der Suhosin-Installation:



Suhosin Extension is up to date!  
Suhosin Patch is up to date!

---

Simulationsmodus ist **eingeschaltet**, zum ausschalten Schalter betätigen.



► phpConfigCheck

► Angemeldete Benutzer

► Beliebt

► Neue Beiträge

► Statistiken

# Suhosin – Backend module

Option	Wert
suhosin.apc_bug_workaround	<input type="text" value="1"/>
suhosin.cookie.checkraddr	<input type="text" value="0"/>
suhosin.cookie.cryptdocroot	<input type="text" value="1"/>
suhosin.cookie.cryptkey	<input type="text"/>
suhosin.cookie.cryptlist	<input type="text"/>
suhosin.cookie.cryptraddr	<input type="text" value="0"/>
suhosin.cookie.cryptua	<input type="text" value="1"/>
suhosin.cookie.disallow_nul	<input type="text" value="1"/>
suhosin.cookie.disallow_ws	<input type="text" value="1"/>
suhosin.cookie.encrypt	<input type="text" value="1"/>
suhosin.cookie.max_array_depth	<input type="text" value="50"/>
suhosin.cookie.max_array_index_length	<input type="text" value="64"/>
suhosin.cookie.max_name_length	<input type="text" value="64"/>
suhosin.cookie.max_totalname_length	<input type="text" value="256"/>
suhosin.cookie.max_value_length	<input type="text" value="10000"/>



# Security tests: OWASP-Top Ten Risks

Impact (default)	Countermeasure	Admin Information
3	warning: "Your entry appears suspicious and has been recorded."	1. entry to log file 2. entry to database if component is installed
9	warning: "Your entry appears suspicious and has been recorded."  warning: "The administrator(s) have been informed of your suspicious activity."	1. entry to log file 2. entry to database if component is installed 3. sending email
27	warning: "Your entry appears suspicious and has been recorded."  warning: "The administrator(s) have been informed of your suspicious activity." warning: "Further suspicious activities will result in a heightened response." (default) error: admin defined message on separate error page (if set) url: redirect to admin defined url (if set)	1. entry to log file 2. entry to database if component is installed 3. sending email

# Security tests: OWASP-Top Ten Risks

50	warning: "Your entry appears suspicious and has been recorded."  warning: "The administrator(s) have been informed of your suspicious activity." warning: "Further suspicious activities will result in a heightened response." logout: in case of an authenticated user	1. entry to log file 2. entry to database if component is installed 3. sending email
100	warning: "Your entry appears suspicious and has been recorded."  warning: "The administrator(s) have been informed of your suspicious activity." warning: "Further suspicious activities will result in a heightened response." (default) ban: in case of an authenticated user, the username will be banned ban: in case of an un-authenticated user, the ip + session will be banned	1. entry to log file 2. entry to database if component is installed 3. sending email

# Security tests: OWASP-Top Ten Risks

#	Exploit	Joomla!	IDS / IPS	Suhosin
1.	Injection	✗	✓	✗
2.	Cross-Site Scripting (XSS)	✓	✓	✗
3.	Broken Authentication and	✓	✗	✗
	Session Management			
4.	Insecure Direct Object	✓	✗	✗
	References			
5.	Cross-Site Request Forgery (CSRF)	✓	✗	✗
6.	Security Misconfiguration	✓	✗	✓
7.	Insecure Cryptographic Storage	✓	✗	✓
8.	Failure to Restrict URL Access	✓	✗	✗
9.	Insufficient Transport Layer	✓	✗	✗
	Protection			
10.	Unvalidated Redirects and Forwards	✓	✗	✗

# Livedemo

- \* Giessen Aegis
- \* Suhosin

# Conclusion

- \* Status:
  - \* Nearly ready to use
  - \* Used on a test server
    - \* <http://www-test.mni.fh-giessen.de/administrator/index.php>
    - \* <http://www-test.mni.fh-giessen.de/>
    - \* Only available from inside the faculty network (also via [VPN](#))
- \* SVN-Repository
  - \* Currently: <http://tracking.mni.fh-giessen.de/svn/joomla/>
  - \* Soon: <http://joomlancode.org/>

# Conclusion

- \* The graphs show that Joomla! Is already protected against most OWASP Risks. But attacks are neither logged, nor countermeasures are executed. The features we developed continues to harden the system and give the administrator a better overview over the current security status of his website.

Thank you for your attention.  
Any questions?

END